Règlementation des cookies

Livre blanc

Sommaire

Audito, société à responsabilité limitée, au capital de 20 000 €
RCS TOULON 808 454 383 00015
Siège social: 865 avenue de Bruxelles, 83500 La Seyne sur Mer
Tél 04 94 11 22 33 - Fax 04 94 11 22 44 - courriel contact@audito.fr - site web www.audito.fr

1. Introduction

Ce guide a pour vocation de vous expliquer pas à pas comment mettre en conformité votre site internet avec la nouvelle réglementation française sur la protection des données personnelles vis-à-vis des cookies, et vous indique les pièges à éviter et quelques astuces pour garantir toujours plus de transparence et de protection à vos visiteurs.

Pour proposer un site internet riche en contenus et en fonctionnalités, vous vous appuyez sur des acteurs internet externes à votre site comme des prestataires de mesure d'audience ou des réseaux sociaux. Ces acteurs externes interagissent avec votre site pour offrir leurs services.

Il y a différents moyens pour les connecter à votre site. Ce peut être un moyen neutre et visible pour l'internaute comme un hyperlien. Il renvoie vers une nouvelle page sans installer de fichiers ou communiquer des données mise à part celles nécessaires pour relier les deux sites. Cependant, l'hyperlien ne vous permet pas d'activer une fonctionnalité ou une application directement à partir de votre site. Pour ce faire, le visiteur doit quitter votre page et aller sur celle de destination de l'hyperlien.

Un autre moyen est de relier le site par un cookie, c'est-à-dire un fichier texte que l'acteur externe a placé, via votre site, sur le disque dur de l'internaute qui le visite. Bien plus riche que l'hyperlien, il peut activer des fonctionnalités directement à partir de votre site, sans avoir à le quitter. En permettant la mise en place de ces fonctionnalités comme par exemple un outil de mesure d'audience, **vous autorisez le fournisseur de cette fonctionnalité d'utiliser votre site internet pour placer ce cookie sur le disque dur de l'internaute**.

Le cookie comporte un identifiant unique qui permet d'enregistrer les actions d'un internaute. Ainsi, si l'ordinateur est utilisé par plusieurs personnes avec chacune un compte propre, le cookie installé pourra obtenir des informations personnelles bien plus fines sur chaque personne qu'il identifiera séparément. Il stocke des informations attachées à la navigation de l'internaute en rapport avec votre site. Les informations stockées peuvent être l'adresse IP de l'ordinateur de l'internaute, l'historique de navigation, le nombre de pages visitées, le nom du serveur qui l'a déposé, une date d'expiration, une page ou une image d'un produit qui a été visualisée, une adresse mail si elle est renseignée, les endroits où il a cliqué sur la page, etc.

Ces informations peuvent uniquement être déchiffrées par celui qui a déposé le cookie.

Prenons un exemple concret :

*En utilisant l'outil de mesure d'audience **Google Analytics**, Google dépose un cookie via votre site internet. Cet outil vous permet d'obtenir des statistiques sur la fréquentation de votre site. Pour ce faire, vous avez autorisé Google à collecter des données grâce au cookie. Selon les règles de confidentialité de Google Analytics ces données ne sont, par défaut, pas anonymes[1]. Cependant, vous n'avez aucun moyen d'accès ou de contrôle pour savoir quels types de données Google a recueilli et dans quel but, hormis les quelques informations que Google émiette le long de ses pages. Est-ce que ce sont celles strictement nécessaires aux statistiques de votre site ou Google poursuit-il un autre objectif comme la commercialisation de ces données ?[2]*

En lisant les règles de confidentialité de Google qui s'appliquent de manière uniforme à tous les pays du monde et à tous les services proposés par l'entreprise, notamment à Google Analytics mais aussi à sa régie publicitaire, Google Advertising, le doute est réel.

[1] Règles de confidentialité à jour du 31/03/2014: https://support.google.com/analytics/answer/6004245?hl=fr

[2] http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/D2013-174__13_juin_2013_Bureau_Publication_Societe_GOOGLE_INC.pdf

C'est aussi l'avis des autorités de contrôle Européennes qui condamnent régulièrement Google pour la violation de la réglementation sur les données personnelles[3]. La CNIL[4] reproche à Google Analytics de récolter des données qui n'ont pas été anonymisées, c'est-à-dire qui permettent d'identifier une personne physique particulière et même de la localiser précisément. Toutefois, l'outil Google Analytics vous soumet des statistiques qui semblent anonymes et générales. ***Qu'a-t-il fait de ces données identifiantes ?***

Si l'on y regarde de plus près, lorsque vous utilisez un service de Google, celui-ci vous impose de créer un compte par lequel vous lui donnez accès à toutes les données et les contenus ayant un rapport direct ou indirect avec vous[5]. En effet, les données et contenus collectés ne sont pas limitativement énumérés mais décrits de manière générale. Officiellement Google affirme que c'est pour vous protéger des risques de failles de sécurité et améliorer ses services et qu'il ne transfère ces données à des tiers qu'avec votre consentement[6]. Or, à aucun moment votre consentement n'est réellement demandé puisque si vous envisagez de refuser, la seule option qu'il vous reste est de ne pas utiliser Google. Concrètement, l'hégémonie des services de Google sur Internet rend ce refus impossible à mettre en œuvre. Vous êtes donc contraint d'accepter ou de vous déconnecter totalement d'Internet.

Ainsi, a contrario, vous donnez carte blanche à Google pour exploiter toutes les données qui vous appartiennent directement ou qui transitent via votre compte. Google Analytics (le service qui vous intéresse à l'origine) peut ainsi les partager avec ses autres services comme ***Google AdSense*** *ou* ***DoubleClick****, ses régies publicitaires, et ainsi monétiser les données personnelles récoltées. C'est la raison pour laquelle vous voyez des publicités sur toutes les pages mêmes les plus intimes de votre compte mail.*

Les éditeurs de cookie transfèrent donc des données collectées à leurs propres filiales ou à leurs propres services et prétendent qu'ils ne violent pas la réglementation française puisqu'ils ne transmettent pas à des tiers.

Cette affirmation est fausse. Tout d'abord, s'agissant des filiales : Une filiale est une entité juridiquement indépendante de la société mère avec laquelle elle entretient seulement des liens financiers et de contrôle. En aucun cas, la personnalité juridique d'une filiale ne peut être confondue avec sa société mère, même si elle est détenue à 100% par la mère. Ainsi, une filiale de Google est un tiers qui ne peut pas recevoir de données collectées sans que vous en ayez expressément connaissance et approuvé ce transfert.

Concernant le partage des données collectées avec d'autres services de l'éditeur de cookie en cause à l'intérieur de la même entité : La réglementation française impose aux personnes qui collectent des données de préciser les finalités de leurs collectes et aux internautes de donner leur consentement pour chaque finalité. En permettant une exploitation de principe pour tous les services des données collectées, l'éditeur de cookie ne respecte pas la réglementation française.

En quoi cela vous concerne-t-il ?

Reprenons l'exemple de Google Analytics. Lors de votre adhésion, vous l'avez autorisé à se servir de votre site internet pour déposer un cookie sur le disque dur de vos internautes et collecter des données à partir de votre site. Maintenant que vous connaissez les dessous du modèle économique de Google et ses méthodes de collecte de données personnelles, sachez que, selon la loi Informatique et Libertés**, vous êtes aussi juridiquement responsable de ce que**

[3] http://www.cnil.fr/linstitution/actualite/article/article/la-formation-restreinte-de-la-cnil-prononce-une-sanction-pecuniaire-de-150000-EUR-a-lencontre/

[4] CNIL : Commission Nationale Informatique et Libertés

[5] https://www.google.fr/intl/fr/policies/privacy/#infocollect

[6] https://www.google.fr/intl/fr/policies/privacy/#infocollect

Google Analytics a recueilli grâce à votre intermédiaire, même si vous n'en connaissez ni le contenu ni toutes les utilités.[7]

Nous vous avons fait la démonstration avec Google mais la problématique est identique, voire plus intrusive, avec la majorité des autres acteurs externes, et en particulier les plus connus comme **Facebook**, **Twitter**, **Conversant**, etc.

C'est le revers de la médaille de la gratuité. Rien n'est jamais gratuit ou à prix modique…

En effet, une fois les données recueillies à partir de votre site, ces éditeurs de cookie peuvent ensuite les mettre en corrélation, avec des informations qu'ils ont obtenues via d'autres sources. Ainsi, en croisant toutes ces données, ces acteurs externes peuvent déterminer les centres d'intérêts de l'internaute en les déduisant de sa navigation. En d'autres termes, ils élaborent un **profil virtuel**, le plus précis possible sur la vie personnelle de l'internaute et l'utilisent pour proposer un service personnalisé à votre besoin et/ou à celui du visiteur de votre site, suggérer un ordre de choix de produits, la mise en relation avec un groupe sur un réseau social mais aussi pour le revendre au plus offrant...
En reprenant notre exemple de Google Analytics qui couvre 96% des sites internet en Union Européenne, combien valent votre profil à ses yeux et à combien de personnes a-t-il revendu vos petits penchants?

Prises séparément, ces informations ne permettent pas de s'introduire dans la vie personnelle de l'internaute. **C'est leur exploitation et leur croisement qui porte atteinte à la vie privée de l'internaute car ils permettent d'établir l'identité d'une personne physique.[8] Pourtant, sans ce croisement d'informations, les services de ces acteurs ne sont pas utilisables.** Le croisement de ce type d'informations n'est pas illégal, si l'internaute qui les a émises a autorisé leur recueil et leur utilisation. La loi ne cherche pas à empêcher le développement de cette pratique. Au contraire, c'est tout l'enjeu des phénomènes "Big Data" et "Open Data". La loi veut seulement garantir une pratique éthique et respectueuse des droits fondamentaux de l'individu.

Toutefois, à la différence des hyperliens, identifiables par l'adresse de destination lorsqu'on positionne le curseur dessus, la présence de cookies n'est pas directement reconnaissable par l'internaute. Dans sa grande majorité, l'internaute n'a même pas conscience de l'utilisation de cookies sur le site qu'il visite.

C'est pourquoi la Loi "Informatique et Libertés" exige de l'éditeur du site d'informer ses visiteurs des cookies présents sur le site, de leur finalités et d'obtenir leur autorisation pour exploiter les données qu'ils vous mettent gracieusement à disposition.

Les risques encourus en cas de violation de la réglementation

Les fournisseurs de services de communications électroniques au public (Fournisseurs d'accès à internet, de téléphonie mobile) ont une obligation de notifier dans les 24 heures à la CNIL les violations du droit sur la protection des données personnelles de sites internet.[9] De plus, la CNIL a un pouvoir de contrôle à distance et de sanction pour les violations du droit sur la protection des données personnelles.[10] Elle-même comme la DGCCRF peuvent infliger les sanctions administratives, voire pénales suivantes :

---

7 Article 3 de la Délibération n° 2013-378 du 5 décembre 2013

8 http://etudiant.lefigaro.fr/les-news/actu/detail/article/des-banques-scrutent-les-profils-facebook-avant-d-accorder-un-credit-2612/;http://www.wsj.com/news/articles/SB10001424052748704648604575620750998072986?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052748704648604575620750998072986.html

9 article 34 Bis, Loi 78-17 du 6 janvier 1978 « Informatique et Libertés », article L33-1 , Code des Postes et Communications électroniques

10 article 45 à 47, loi 78-17 « Informatique et Libertés »

Montant des sanctions :

Tous les sites: article 47 loi Informatique et Libertés:
Retrait de l'autorisation de traitement des données
Fermeture du site jusqu'à 3 mois
Publicité des sanctions prononcées
Amende jusqu'à **150 000 €** pour chaque infraction
Si récidive amende jusqu'à **300 000 €** pour chaque récidive
Si entreprise jusqu'à **5% du CA h.t.** du dernier exercice clos dans la limite de **300 000€** pour chaque infraction

Sanctions pénales article 226-18 du Code pénal :
5 ans d'emprisonnement
300 000 € d'amende
Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite.
Implanter un cookie dans un terminal à l'insu de l'internaute est considéré comme déloyal.

Sanctions complémentaires pour sites marchands article L111-1 et L111-6 du Code de la Consommation:
Amende administrative jusqu'à **3 000 €** par infraction pour une personne physique
et jusqu'à **15 000 €** par infraction pour une personne morale

Votre site n'est pas à l'abri non plus des poursuites judiciaires de particuliers ou de campagnes de dénigrement en ligne qui peuvent apporter une très mauvaise publicité à votre entreprise et vous faire perdre beaucoup de chiffre d'affaires.

Ce guide va ainsi vous expliquer pas à pas et de manière personnalisée comment mettre en conformité votre site internet avec la nouvelle réglementation sur les cookies.

2. Apprendre à connaître les cookies

« Les cookies sont de petits enregistrements déposés sur votre disque dur par le site visité, lui permettant de vous reconnaitre lors d'une prochaine visite, et de stocker certaines informations vous concernant. Pris au sens large, un cookie couvre l'ensemble des traceurs déposés et / ou lus, par exemple, lors de la consultation d'un site internet, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel ou d'une application mobile. La loi s'applique quel que soit le type de terminal utilisé et concerne par exemple, les traceurs déposés sur les ordinateurs, smartphones, tablettes numériques et consoles de jeux vidéo connectées à Internet. Par commodité, nous utilisons le terme de "cookie" qui recouvre l'ensemble de ces technologies »[11].

L'article 29 de la loi Informatique et libertés, la délibération de la Commission nationale de l'Informatique et des Libertés du 5 décembre 2013 et la directive européenne du 1995 applicables, disposent que tout traitement automatisé d'une donnée à caractère personnelle nécessite l'accord de son propriétaire.

11 http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/

Une donnée à caractère personnelle est **toute information concernant une personne physique identifiée ou identifiable. Est réputée identifiable toute personne qui peut être identifiée, directement ou indirectement, par référence à un ou plusieurs éléments spécifiques propres à son identité physique.[12] En d'autres termes, une donnée personnelle n'est pas une information à proprement parlé identifiante, tel qu'un nom, un prénom, une adresse, etc. mais il peut s'agir d'éléments semblant neutres qui, mis bout à bout, permettent d'identifier une personne physique. C'est justement tout le problème des informations stockées par les cookies.**

Un traitement de données est quant à lui le « liant » qui va « faire parler » les données et leur donner un sens pour un objectif précis. Ainsi, la Loi Informatique et Libertés défini le traitement comme suit :

« Toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »[13]

En conséquence, même un algorithme, peut tomber sous le champ d'application de la loi, puisqu'il permet l'articulation et l'organisation des données collectées.

Un doute si le support que vous utilisez entre dans le cadre de la loi Informatique et Libertés ? Votre fichier informatique, peu importe sa forme, que ce soit un fichier, Word, Excel, votre agenda sur Google, les données disponibles sur votre moteur de recherche, tombent bien sous le couvert de la loi Informatique et Libertés, puisqu'un fichier consiste en « t*out ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés. »*[14]

En conséquence, les informations à caractère personnel ne sont librement disponibles ni dans leur accès ni dans leur traitement. L'accord de l'internaute est nécessaire pour stocker les informations le concernant sur un cookie et les exploiter. Cela vaut aussi pour les informations personnelles qui semblent publiquement accessibles sur votre moteur de recherche. Ce n'est pas parce que vous pouvez y accéder facilement que vous avez le droit de le faire.

Prenons un exemple concret :

Vous marchez le long de la rue et la maison à votre droite a sa fenêtre du rez-de-chaussée grande ouverte. Vous pouvez donc facilement entrer chez son habitant inconnu. Vous a-t-il pour autant invité à entrer chez lui ? Oseriez-vous entrer dans sa maison et commencer à fouiller dans ses tiroirs à son insu pour connaître sa vie privée ? De surcroît, vous compter revendre aux publicitaires les plus offrants les informations que vous récoltez suite à cette fouille. Des publicités et des appels téléphoniques envahiront alors ce malheureux habitant.

Inimaginable pour toute personne respectable, alors pourquoi cette impunité sur internet ?

La réglementation sur les cookies permet justement à l'internaute d'être informé sur cette pratique et d'avoir l'opportunité de s'y opposer. Pour donner un accord éclairé, l'internaute a besoin de savoir quelles informations sont recueillies sur lui, par qui et dans quel but elles seront exploitées.

12 Article 2 de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « Informatique et libertés »
13 Article 2 de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « Informatique et libertés »
14 Article 2 de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « Informatique et libertés »

Ainsi lorsque l'internaute accède à votre site, si les informations qu'il vous transmet sont uniquement exploitées par votre site dans le seul but de permettre son bon fonctionnement, vous n'avez pas besoin d'accord de l'internaute, une information sur la présence de ces cookies est suffisante. Pour les autres applications ou modules intégrés qui n'appartiennent pas au site et ayant une finalité différente, un accord est nécessaire et vous devez indiquer dès le premier accès sur le site une information sur la présence de ces types de cookies.

Résumé sur les cookies soumis à accord :

Soumis à accord: tous les cookies de tiers ayant pour finalité :

- Publicitaire
- Traceur (traque l'internaute au cours de sa navigation sur des sites tiers)
- Accès à un réseau social (envoi d'informations à des réseaux sociaux)
- Analytique (mesure d'audience, analyse de la navigation sur le site)

Exemptés d'accord:

- De fonctionnement du site
- Nécessaire pour répondre à une demande expresse de l'internaute (ex: panier d'achat, paiement, récupérer l'accord de l'internaute, etc.)

Exemptés sous condition d'information:

PIWIK ANALYTICS pour la mesure d'audience

Comment identifier les cookies que vous hébergez sur votre site ?

Recensez tous vos e-partenariats

C'est-à-dire tous les accords, conventions et contrats que vous avez conclus avec des tiers et qui ont nécessité la modification des codes sources de votre site internet, par exemple en y ajoutant une nouvelle ligne de code.

Faites une analyse de vos entêtes de requêtes avec HTTP HEADERS

Ce petit logiciel librement disponible et gratuit permet d'analyser en profondeur toutes les requêtes envoyées depuis votre site internet. Il permet ainsi d'identifier les cookies de tiers qui ont vocation à s'installer depuis votre site.

Astuce :

Le marché de l'édition des cookies est très riche et il existe beaucoup d'acteurs français. Apprenez à bien choisir vos cookies et méfiez-vous de l'installation standard de vos modules. Lorsque vous choisissez votre module, vérifiez l'origine de l'exploitant (membre de l'Union Européenne ou pas), sa fiabilité (par exemple s'il est un adhérent actif de la convention « Safe Harbor »), ses options et modalités de confidentialité, la sécurité du protocole de transfert d'informations, la durée de vie de ses cookies. En effet, certains modules, même gratuits, comme Google Analytics, vous proposent d'installer en option (gratuite) une application qui « anonymise » les adresses IP avant leur stockage sur son cookie. Cela ne vous libère toujours pas de vos responsabilités mais limite un peu les risques. En

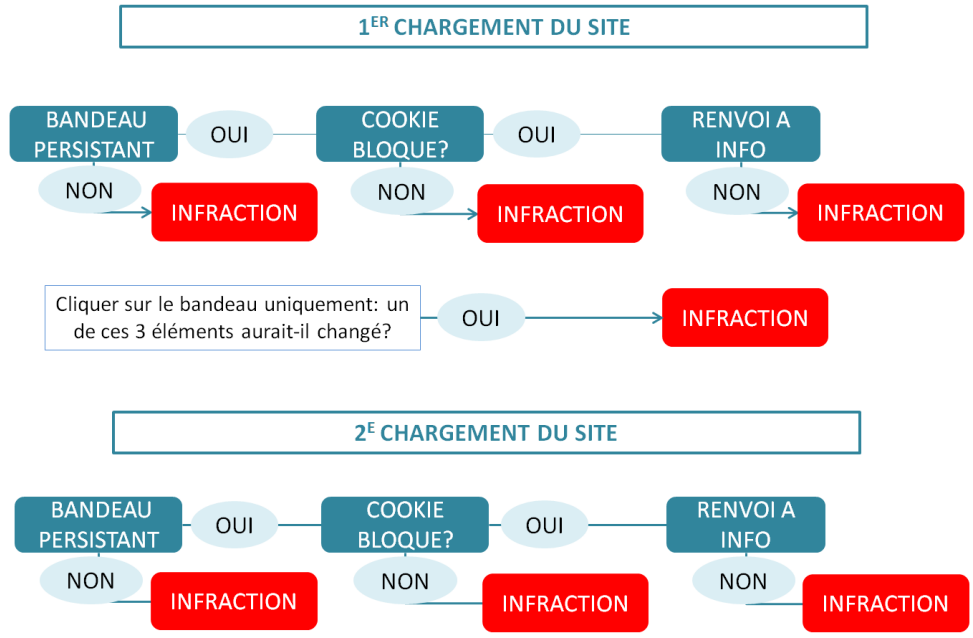
privilégiant les éditeurs de cookie européens, vous limitez aussi l'imprévisibilité dans l'engagement de votre responsabilité juridique à cause d'une législation que vous ne maitrisez pas.

*D'ailleurs, l'utilisation par les internautes de modules destinés à bloquer des cookies comme **GHOSTERY** ou **ADBLOCK** ne vous libère pas de votre responsabilité et ne vous garantit pas qu'un cookie n'ait été installé. En effet, principalement américains, ils identifient très bien les cookies d'éditeurs américains mais connaissent rarement les cookies d'éditeurs européens. De plus, ces modules ont souvent aussi comme modèle économique la revente de données personnelles*

3. Obligations d'information

Premier accès

Contrairement à la pratique générale, au moment du premier accès sur le site, les cookies nécessitant l'accord de l'internaute doivent être inactifs ! Un bandeau ou une fenêtre pop-up persistante s'affiche jusqu'à ce que l'internaute ait effectué une action qui exprime son accord ou son désaccord. Si l'internaute quitte votre site sans avoir effectué d'action: Retour à la case départ ; aucun cookie ne pourra s'activer à sa prochaine visite tant qu'il ne se sera pas exprimé.



Astuce :

Nous vous déconseillons l'utilisation d'une fenêtre pop-up qui peut être bloquée selon la configuration du navigateur et s'imbrique moins bien dans l'ergonomie de votre site.

La décision de l'internaute est valable pour une **durée maximale de 13 mois**. Une fois que l'internaute a donné sa décision, le bandeau ou la fenêtre pop-up pourraient ne plus être affichés lors des prochaines visites durant les 13 mois suivants.

Bannière ou pop-up d'information

Le bandeau ou la fenêtre pop-up doit être accessible dès le premier accès de l'internaute sur le site, que ce soit la page d'accueil ou tout autre page. Le bandeau doit indiquer la présence de cookies avec leurs différentes finalités, recueillir l'accord de l'internaute et donner un accès à la politique de gestion des cookies.

Plusieurs méthodes sont possibles pour recueillir l'accord :

- Expressément : Vous intégrez un bouton que l'internaute doit cliquer pour recueillir son accord et déclencher l'activation des cookies,

Exemple de texte :

« Notre site - XXXXXXX - utilise des cookies de fonctionnement et à des fins publicitaire, de mesure d'audience, d'accès aux réseaux sociaux et d'établissement de profils.
Pour accepter l'utilisation de ces cookies, merci de cliquer ci-contre : OUI

Si vous souhaitez en savoir plus et paramétrer vos choix, cliquez ici. »

Bouton débloquant les cookies

Lien actif vers la Politique de gestion des cookies ou CGU

- Implicitement : Les cookies pourront s'activer si l'internaute clique sur le site mais en dehors du bandeau ou de la fenêtre. Si l'internaute clique uniquement sur le bandeau ou la fenêtre pop-up, les cookies doivent rester inactifs.

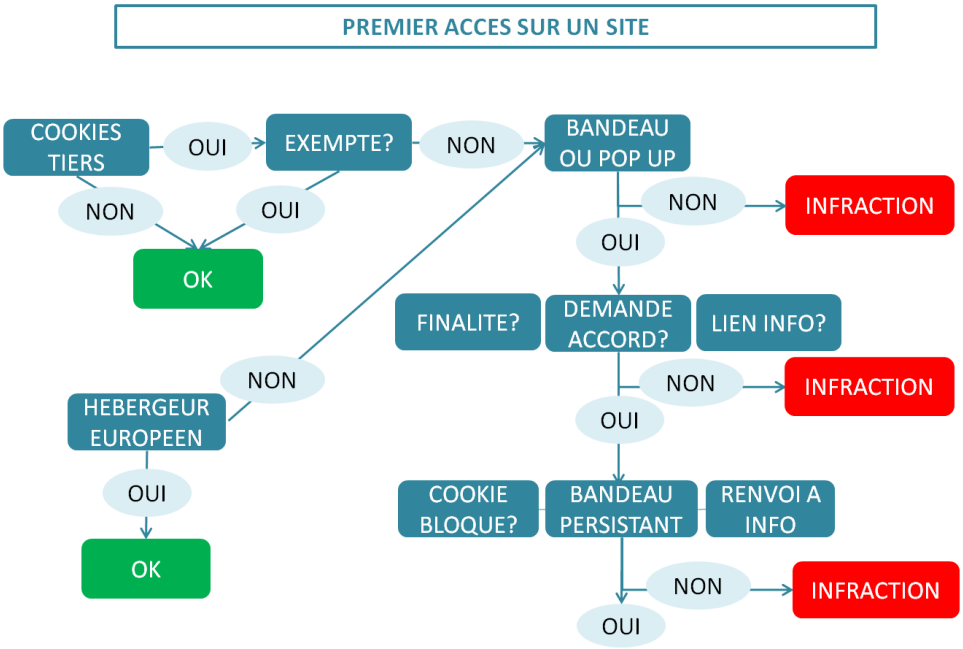
Exemple de texte :

« Notre site - XXXXXXX - utilise des cookies de fonctionnement et à des fins publicitaire, de mesure d'audience, d'accès aux réseaux sociaux et d'établissement de profils. En poursuivant votre navigation, vous acceptez l'utilisation de ces cookies. Si vous souhaitez en savoir plus et paramétrer vos choix, cliquez ici. »

Lien actif vers la Politique de gestion des cookies ou CGU

Astuce :

Pour plus de simplicité dans l'utilisation de votre site tout en satisfaisant les exigences de la réglementation, nous vous conseillons d'opter pour l'obtention tacite de l'accord de l'internaute au niveau du bandeau. L'internaute pourra toujours revenir sur sa décision en allant sur la page de politique de gestion des cookies.



4. Politique de gestion des cookies

Ce que nous appelons *la politique de gestion des cookies* est une page d'information sur les cookies qui comporte des modules permettant à l'internaute d'accepter ou de rejeter des cookies par groupe de finalité.

Accessibilité

La page de politique de gestion des cookies doit être accessible directement depuis le bandeau ou la fenêtre pop-up et facilement depuis le site, par exemple à partir du menu.

Inactivité des cookies

Lorsque l'internaute accède sur le site via le bandeau ou la fenêtre pop-up, sans avoir au préalable exprimé une décision, les cookies doivent être inactifs. Les cookies restent inactifs pendant toute la durée de la visite de cette page d'information, jusqu'à ce que l'internaute ait exprimé son accord.

Informations obligatoires

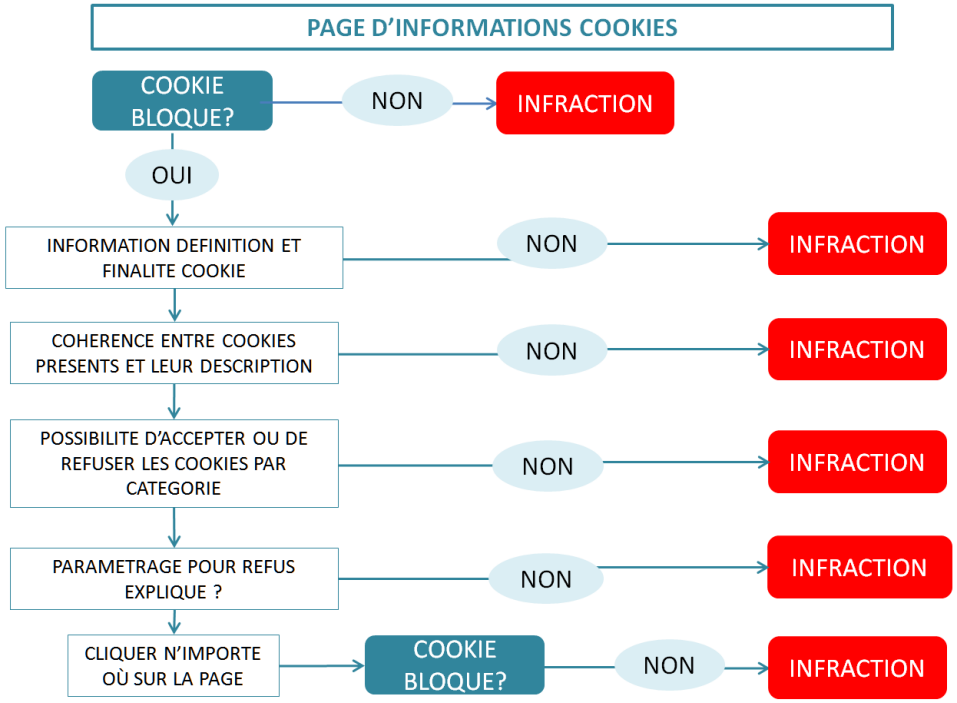
Définition précise de tous les cookies présents sur le site :

- Mention du nom commun du cookie
- Mention du nom du propriétaire du cookie
- Mention si les données sont transférées en dehors de l'Union Européenne et dans le cas d'une entreprise des Etats-Unis d'Amérique si elle est adhérente au programme « Safe Harbor »
- Mention de la durée de vie du cookie et des données collectées
- Mention du type d'informations collectées
- Mention de la finalité du cookie

Exemple sur un bouton de partage :

- *Nom commun du cookie : « J'aime » de Facebook*
- *Propriétaire et exploitant du cookie: Facebook Inc.*
- *Nationalité : États-Unis d'Amérique, adhérent « Safe-Harbor »*
- *Durée de vie cookie : indisponible*
- *Conservation des données : 90 jours*
- *Informations collectées (non exhaustives et sous réserves de modifications par l'exploitant): identifiant d'utilisateur Facebook, données de connexion, nombre fois le bouton a été cliqué, pages visitées, pages cliquées, date et heure des visites,…*
- *Finalité : connexion au réseau social et autres finalités propres à l'exploitant.*

Nous vous invitons à consulter la politique de confidentialité de l'exploitant.



Astuce :

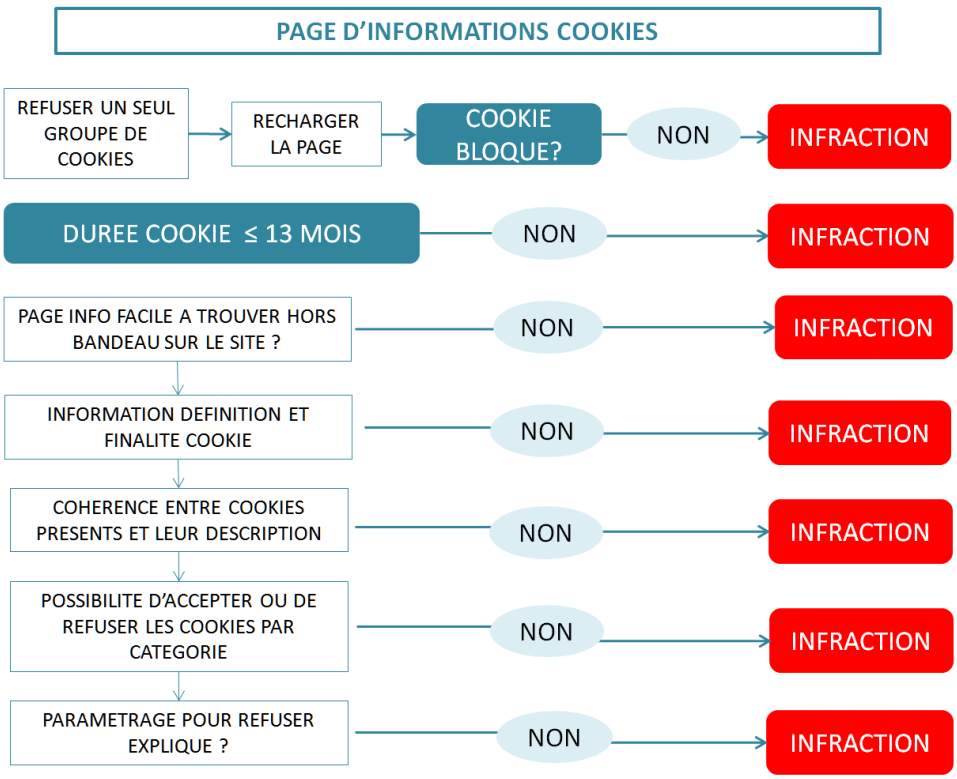
Atténuez votre responsabilité en précisant que vous ne maitrisez pas les informations qui sont collectées ni toutes les finalités de l'exploitant du cookie lorsque ces informations vous sont incertaines ou méconnues. Par exemple, Facebook déclare dans sa politique de confidentialité d'utiliser les données collectées pour connecter les internautes à son réseau social mais aussi à des fins commerciales et techniques propres.

Renvoyez aussi les internautes vers les conditions générales des exploitants. Attention : Elles sont souvent très compliquées et éparses, nous vous déconseillons d'insérer un hyperlien qui mène vers elles car il est source d'écueils et doit être régulièrement mis à jour (renvoi vers les mauvaises conditions, page ou conditions générales obsolètes …).

5. Recueil de l'accord de l'internaute

Peu importe la procédure mise en place, vous devez expliquer à votre visiteur comment il peut accepter ou refuser l'installation de cookies depuis votre site et, en conséquence, la récolte de ses données.

L'internaute doit pouvoir refuser les cookies au moins par groupe de finalité et à partir de cette page d'information. En somme, il doit avoir la possibilité de refuser tous les cookies tiers au site. La CNIL rejette expressément le renvoi à d'autres pages en dehors de votre site internet pour exercer son acceptation ou son refus d'activation de cookies. Elle considère aussi comme insuffisant d'expliquer comment limiter ou bloquer les cookies de tiers via le navigateur.



Exemple :

Veuillez cocher :

Groupe de finalités	Actif	Inactif
Analytique	☐	☑
Réseau social	☑	☐

→ La sélection déclenche l'action d'activation ou de désactivation des groupes de cookies

Astuce :

Pour les boutons de partage des réseaux sociaux, il existe des applications gratuites qui permettent d'activer / désactiver les cookies et d'obtenir le consentement de l'internaute et s'intègrent facilement dans votre site comme **share privacy**.

A ce stade, vous devez garantir strictement les choix de l'internaute. En conséquence, si aucune activation n'a été précédemment demandée, tous les cookies doivent rester inactifs. Si l'internaute choisi d'accepter un groupe de finalités de cookies, voire un cookie en particulier, cela ne peut pas activer les autres cookies de tiers présents sur le site, sauf ceux de fonctionnement qui n'ont pas besoin d'accord.
Les données enregistrées à partir de cette page d'informations doivent être identiques peu importe si l'on accède par la bannière, la fenêtre pop-up, ou le menu du site.

Astuce :

La CNIL tolère de renvoyer les utilisateurs vers des cookies de refus mis en place par les éditeurs de cookies eux-mêmes comme le cookie d'opposition de Google Analytics ou ceux générés par l' « European Digital Interactive Alliance ». Cependant, ils nécessitent quand même une intégration informatique particulière et le paramétrage des cookies pour fonctionner.

En revanche, ces cookies d'opposition ne désactivent pas le cookie avant l'obtention du consentement. Ils agissent uniquement si le cookie est bien paramétré et après que l'internaute ait su correctement l'installer sur son navigateur. Cette démarche est très compliquée même pour un internaute averti et ne vous exonère toujours pas de vos obligations pour les cookies qui ne proposent pas ce type de module.

6. Charte des Bonnes Pratiques pour votre site Internet (à l'usage des experts)

1. Référencez dans les registres officiels et indiquer des mentions légales complètes :
   - ✓ Pas d'identité offusquée dans le registre Whois
   - ✓ Inscrire son nom de domaine au Registre du Commerce et des Sociétés
2. Choisissez des e-partenaires européens ou s'engageant à respecter la loi française (hébergeur, prestataires IAAS, SAAS, CDN, Cloud, e-marketing, etc.)
   - ✓ S'assurer que leurs propres partenaires soient aussi soumis à la réglementation européenne
1. Listez et maintenez à jour les partenaires accédant à des données personnelles via votre site
2. Analysez les vrais besoins en traceurs et mesure d'audience
3. Impliquez vos conseils juridiques ou votre Correspondant Informatique et Libertés dans tous le processus des e-partenaires et travailler en équipe!
4. Considérez la cohérence de l'offre des agences de marketing sur les cookies avec leur discours commercial
5. Pénalisez contractuellement les e-partenaires qui réutilisent les données de vos visiteurs sans votre autorisation expresse
6. Affichez les bannières d'informations avec les finalités, l'obtention du consentement et le renvoi vers fiche explicative
7. Si vous acceptez la monétisation de ces données, informez l'internaute
8. Lors du choix de vos cookies, considérez le niveau de protection des données personnelles du cookie, notamment
   - ✓ Type de technologie utilisée
   - ✓ Durée de vie
   - ✓ Technologie de masquage / anonymisation
   - ✓ Cryptage
9. Indiquez la durée de vie du cookie dans l'entête des requêtes
10. Paramétrez les cookies pour chiffrer, masquer, anonymiser ou limiter la récolte des données personnelles et leur durée de vie
11. Limitez tous les cookies à 13 mois maximum et supprimez les données personnelles après ce délai
12. Retirez les cookies obsolètes ou dont le contrat est terminé
13. Analysez le positionnement du cookie
14. Evitez les cookies publicitaires ou de profilage (éventuellement la mesure d'audience) sur des pages sensibles comme les formulaires de contact, formulaires et tunnels de commande et de paiement…
    - ✓ Evitez le renvoi vers ces pages sensibles ("*referrer"/ "referer")*
    - ✓ Ces pages sensibles doivent éviter tout intermédiaire pour éviter une interception
15. Faites transiter les données de ces pages en SSL /TLS (https) sous protocole POST
16. Evitez que les entêtes des requêtes ou adresses URL contiennent de données personnelles directement identifiantes, comme une adresse mail
17. Cryptez et effacez les données identifiantes (métadonnées) dans les photos et vidéos
18. Adhérez à la Charte Do Not Track, respectez-la et faites-la respecter à vos partenaires

7. Conclusion

Vous avez maintenant toutes les cartes en main pour mettre votre site internet en conformité avec les nouvelles obligations de la CNIL.

Trop compliqué, trop coûteux ou pas le temps de le faire vous-même ?

AUDITO peut le faire pour vous et vous propose une solution complète et pérenne de mise en conformité grâce à son un outil de gestion des cookies simple et intégré à votre site.

*Visitez notre site internet **www.audito.fr** et contactez-nous pour plus d'informations.*